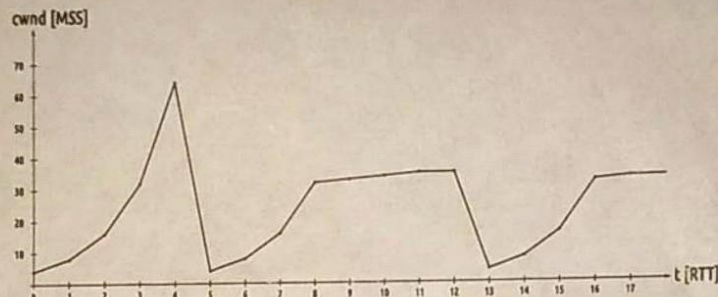


Apellido:	Orden:	Hojas ->	Ej.1	Ej.2	Ej.3	Ej.4	
Nombre:	Calif. ->	Calif. ->	X	B	B	A	Final: A-

Todas las respuestas se consideran válidas solo si están debidamente justificadas.

Ejercicio 1

Dada la imagen representando una conexión TCP donde $MSS = 1KB$. Describa y justifique valores compatibles con la imagen para el $SSThreshold$ y el algoritmo de control de congestión en uso por cada RTT .



Ejercicio 2

Peterson desea mandarle un mail a Tanenbaum. Sus respectivos mails son claudia@peterson.com y ernesto@tanenbaum.com.

1. Describa los registros DNS necesarios en las zonas de dominio peterson.com y tanenbaum.com para que sea posible tanto enviar como recibir el correo. La descarga es por medio de un servidor pop3.
2. Suponiendo que todas las caches de la red están vacías. Detalle los mensajes del protocolo DNS necesarios para que el DNS resolver Stallings, de quien ya se conoce la IP, obtenga una respuesta autoritativa cuando consulta por la IP del servidor de correo de peterson.com mediante una consulta iterativa. La consulta DNS a Stallings es recursiva.

Ejercicio 3

a. Ernesto es popular por su fanatismo para utilizar conexiones Wi-Fi inseguras donde Marquitos suele *sniffearle* los paquetes y robarle información. Dado que Claudia teme que a Martín le llegue el contenido de estos mensajes, es necesario que no puedan ser descifrados por Marquitos pero sí por Ernesto.

- (a) Explique un mecanismo que garantice esta propiedad. ¿Qué información tienen que tener Claudia y Ernesto para que esto sea posible?
- (b) Justifique cuáles aspectos de seguridad (confidencialidad, no repudio, integridad, autenticidad, disponibilidad) se cumplen cada vez que Claudia le envía un email a Ernesto.

Nota: No se puede usar ningún protocolo que corra sobre TLS/SSL.

b. Una empresa debe exponer un servidor HTTP a Internet. También tiene un servidor para recepción y envío de email. Además, cuenta con un servidor SSH que funciona como punto de entrada a la DMZ para luego conectarse a los demás servidores de la misma.

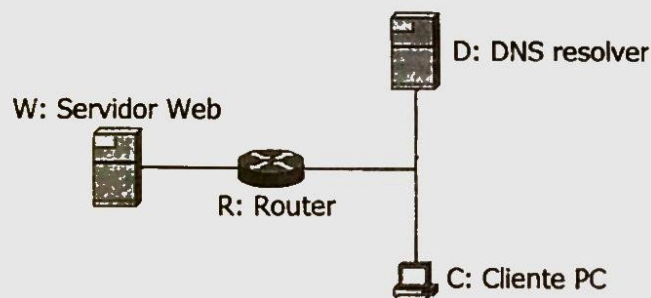
- (a) Diagrame un esquema de conectividad mostrando cómo organizar los servidores en una zona demilitarizada (DMZ) que permita proteger la red de la empresa de atacantes directos usando un firewall *Statefull*.
- (b) Muestre las reglas del firewall, para el diagrama del ítem anterior, teniendo en cuenta que:
- Desde Internet sólo se puede acceder a los servicios de la DMZ.
 - Desde la red interna se permite HTTPS hacia Internet.
 - Desde la red interna se pueden enviar y descargar emails.

Ejercicio 4

Un *host* C de la topología que se muestra abajo quiere descargar la página web <http://www.militohay/unosolo.html> del servidor W. Todos los enlaces son segmentos Ethernet. Se pide detallar (ver tabla) todos los paquetes involucrados en la descarga a partir del momento en que el usuario presiona <enter> en el navegador hasta que los datos le llegan al cliente. Asuma que:

- Todas las máquinas tienen sus cachés ARP vacíos.
- D tiene en su caché DNS los datos correspondientes a www.militohay.
- <http://www.militohay/unosolo.html> "entra" en un único paquete.
- El cliente acaba de ingresar a la red, de tal manera que todas sus cachés están vacíos (HTTP, DNS, ARP, etc.).
- Se está corriendo una implementación de TCP "básica", tal que no está haciendo ninguna optimización del tipo de retrasar ACKs o piggybacking.

Si el encabezado de un paquete cambia durante la transmisión (i.e., la dirección IP o la dirección MAC cambia), debería escribir el paquete en dos líneas separadas, correspondientes a los dos conjuntos de headers que se ven durante la transmisión. Notación: PROTOCOLO [TIPO] [(ORIGEN, DESTINO)]. Nota: Indicar Broadcast como "BR".



Orden	Aplicación	Transporte	Red / Aux	Enlace
1				
2				
3				
...				
...				
...				
n-1	HTTP Reply	TCP (PORT-W, PORT-C)	IP (IP-W, IP-C)	ETH (MAC-W, MAC-R)
n	HTTP Reply	TCP (PORT-W, PORT-C)	IP (IP-W, IP-C)	ETH (MAC-R, MAC-C)